ICS 2O0
Unit 1 - Hardware

Worksheet – Computer Security

There have been *many* famous viruses and worms over the years. Choose 5 (five) to research and give a brief summary about them including how they were used, how much damage (if any) they caused, and how they spread (if applicable).

Here are some good links to get you started:

10 Most Destructive Computer Viruses – Hongkiat:
http://www.hongkiat.com/blog/famous-malicious-computer-viruses/

Top Ten Most-Destructive Computer Viruses – Smithsonian
http://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/?no-ist

Save a copy of your answers to the Google drive!

Virus/Worm #1:
ILOVEYOU was a virus that damaged many computer system worldwide. ILOVEYOU caused a damage of estimated $10 Billion. ILOVEYOU virus was spread through outlook email attachments subject I Love You and when a user would click on that email the virus would spread and it would also delete some files and data from the computer.

Virus/Worm #2:
Melissa was a virus that was in an infected word document, this word document was on a pornographic site claiming to have passwords for the pornographic sites. This got many people curious therefore they clicked on it and the virus would spread in the computer and it would sent itself to 50 other people causing a great traffic of this virus and affecting other document and files in the computer. This virus caused a damage of $80 Million.

Virus/Worm #3:
Zeus is a trojan horse made to effect windows computer in order to perform numerous criminal tasks. Zeus was used to do many criminal tasks, but it was mainly used to steal banking information by man-in-the-browser keystroke logging and form grabbing. Zeus caused a damage of $70 Million. Zeus was spread through drive-by-downloads or phishing scams.

Virus/Worm #4:

Conficker was a worm infection that infects computers using flaws in the Operating System to create a botnet. Conficker caused an estimated total damage of $9 Billion. The worm works by exploiting a network service vulnerability that was present and unpatched in Windows. Once infected, the worm will then reset account lockout policies, block access to Windows update and antivirus sites, turn off certain services and lock out user accounts among many. Then, it proceeds to install software that will turn the computer into a botnet slave and scareware to scam money off the user. Microsoft later provided a fix and patch with many antivirus vendors providing updates to their definitions.

Virus/Worm #5:

Stuxnet was a virus that was created for the purpose of cyberwarfare. The computer worm was designed to attack industrial Programmable Logic Controllers (PLC), which allows for automation of processes in machinery. Stuxnet was entered VIA a USB stick causing to spread to other computers through the network.